4

	Notice of Allowability	Application No.	Applicant(s)
		09/937,120	ASANO ET AL.
		Examiner	Art Unit	
		Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *phone interview on 7/12/2007*.

2. ☒ The allowed claim(s) is/are *1,4-9,12-16,19,22-26,29-33,36,39-43,46,179 and 181*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some*   c) ☐ None   of the:

        1. ☒ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *7/12/2007* .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/2/2007 has been entered.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Andrew T. Didel (Reg. No. 45,256) on 7/12/2007.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 2 – 3, 10 – 11, 17 – 18, 20 – 21, 27 – 28, 34 – 35, 37 – 38, 44 – 45, 47 – 178, 180 and 182 without prejudice.

Replace claim 1, 19, 36 and 46 as follows.

Claim 1:

A data processing apparatus for processing content data provided by a recording or communication medium, said apparatus comprising:

a cryptography process section for executing a cryptography process on said content data; and

a control section for executing control for said cryptography process section, wherein said cryptography process section is configured to:

split a first portion of header data of the content data having data on usage policy into a plurality of first messages, said header data including a first stored check value therein,

generate a first integrity check value or values from a first key stored in said cryptography process section to verify integrity of the header data by using said plurality of first messages,

collate said first integrity check value or values to verify said first portion of the header data including the usage policy by comparing said first integrity check value or values to said first stored check value,

split a second portion of the header data of the content data having a content key into a plurality of second messages, said header data including a second stored check value therein,

generate a second integrity check value or values from a second key stored in said cryptography process section to verify integrity of the header data by using said plurality of second messages, wherein said second integrity check value or values is generated by applying the second key to a block information table key, the content key and a block information table,

collate said second integrity check value or values to verify said second

portion of the header data including a said block information table by comparing said

second integrity check value or values to said second stored check value,

generate an intermediate integrity check value based on said first integrity

check value or values and said second integrity check value or values, and

use said intermediate integrity check value to verify said content data corresponding to

said first and second integrity check values.

Claim 19:

A data processing method for processing content data provided by a

recording or communication medium, said method comprising:

splitting a first portion of header data of the content data having data on

usage policy into a plurality of first messages, said header data including a first stored

check value therein;

generating first integrity check value or values from a first key to verify

integrity of the header data by using said plurality of first messages;

collating said first integrity check value or values to verify said first portion

of the header data including the usage policy by comparing said first integrity check

value or values to said first stored check value;

if said first portion of the header data is verified, splitting a second portion

of the header data of the content data having a content key into a plurality of second

messages, said header data including a second stored check value therein;

generating second integrity check value or values from a second key to

verify integrity of the header data by using said plurality of second messages, wherein

said second integrity check value or values is generated by applying the second key to a block information table key, the content key and a block information table;

collating said second integrity check value or values to verify said second portion of the header data including a said block information table by comparing said second integrity check value or values to said second stored check value;

if said second portion of the header data is verified, generating an intermediate integrity check value based on said first integrity check value or values and said second integrity check value or values; and

verifying said content data corresponding to said first and second integrity check values using said intermediate integrity check value.

Claim 36:

A data verifying value imparting method for a data verifying process, said method comprising:

splitting a first portion of header data of data having data on usage policy into a plurality of first messages, said header data including a first stored check value therein;

imparting first integrity check value or values by using said plurality of first messages and a stored first key;

comparing said first integrity check value or values to said first stored check value to verify a usage policy of said header data;

if said usage policy is verified, splitting a second portion of the header data of the data having a content key into a plurality of second messages, said header data including a second stored check value therein;

imparting second integrity check value or values by using said plurality of second messages, wherein said second integrity check value or values is generated by applying a second key to a block information table key, the content key and a block information table;

comparing said second integrity check value or values to said second stored check value to verify a said block information table of said header data; and

if said block information table is verified, imparting an intermediate integrity check value to data to be verified, said intermediate integrity check value being used to verify content data corresponding to said first integrity check value or values and said second integrity check value or values.

Claim 46:

A recording medium recorded with a computer program for executing a data verifying process having certain actions, said actions comprising:

splitting a first portion of header data of data having data on usage policy into a plurality of first messages, said header data including a first stored check value therein;

executing a collation process using a first integrity check value or values generated by using said plurality of first messages and a stored first key, including comparing said first integrity check value or values to said first stored check value to verify a usage policy of said header data;

if said usage policy is verified, splitting a second portion of the header data of the data having a data key into a plurality of second messages, said header data including a second stored check value therein;

executing a collation process using a second integrity check value or values generated by using the plurality of second messages, including comparing said second integrity check value or values to said second stored check value to verify a block information table of said header data, wherein said second integrity check value or values is generated by applying a second key to a block information table key, the content key and said block information table; and

if said block information table is verified, using an intermediate integrity check value to verify said content data corresponding to said first and second integrity check values, said intermediate integrity check value being based on an integrity check value set obtained by combining at least some of said first and second integrity check values together.

Allowable Subject Matter

1. Claims 1, 4 – 9, 12 – 16, 19, 22 – 26, 29 – 33, 36, 39 – 43, 46, 179 and 181 are allowed.

2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims 1, 19, 36 and 46 (& associated dependent claims).

The prior arts fail to teach or suggest data processing apparatus configured to split a first portion of header data of the content data having data on usage policy into a plurality of first messages, the header data including a first stored check value therein, generate a first integrity check value or values from a first key stored in the

cryptography process section to verify integrity of the header data by using the plurality of first messages, collate the first integrity check value or values to verify the first portion of the header data including the usage policy by comparing the first integrity check value or values to the first stored check value, split a second portion of the header data of the content data having a content key into a plurality of second messages, the header data including a second stored check value therein, generate a second integrity check value or values from a second key stored in the cryptography process section to verify integrity of the header data by using the plurality of second messages, wherein the second integrity check value or values is generated by applying the second key to a block information table key, the content key and a block information table, collate the second integrity check value or values to verify the second portion of the header data including the block information table by comparing the second integrity check value or values to the second stored check value, generate an intermediate integrity check value based on the first integrity check value or values and the second integrity check value or values, and use the intermediate integrity check value to verify the content data corresponding to the first and second integrity check values.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.
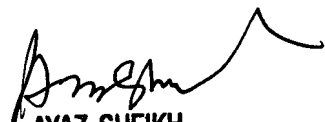
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai

Examiner

Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100